REMARKS

Claims 1-53 are pending in the application, and were each rejected.

Please note that, for ease of reference, all references to the instant application use the paragraph numbers as shown in the published version of the application (US 2003/0156715).

CLAIM REJECTIONS -- 35 U.S.C. §101

Claims 33-48 were rejected under 35 U.S.C. 101, alleging that the claimed invention is directed to non-statutory subject matter. This rejection is traversed.

Claims 33-40 are directed to a receiver, which is a which is specific hardware device (which can utilize software components), an article of manufacture, and a machine. A receiver is clearly statutory subject matter. The instant application describes in [0019]:

> The receiver 112 in the remote unit 110 includes a controller 120 in addition to analog circuitry 122 such as antennas, amplifiers, mixers, control circuits and other components. The controller 120 may be a processor, microprocessor or any other processor arrangement or combination suitable for running software code that facilitates the overall functionality of the remote unit 110 in addition to the decryption and receiver functions described herein. The controller 120, for example, may facilitate the operation of the transmitter 114 in addition to other tasks in the remote unit 110.

Similarly, claims 41-47 are directed to a transmitter, which is a which is specific hardware device (which can utilize software components), an article of manufacture, and a machine. A transmitter is clearly statutory subject matter. The instant application describes in [0018]:

> In addition to analog circuitry 116 such as antennas, amplifiers, mixers, control circuits and other components, the transmitter 106 within the base station 104 includes a controller 118 such as a processor, microprocessor or any other processor arrangement. Software code running on the controller 118 facilitates the overall functionality of the transmitter 106 in addition to the encryption and transmission functions described herein. As is known, circuitry within the transmitter 106 may be implemented as part of the receiver 108.

As such, claims 33-48 are all clearly directed to statutory subject matter. Though they include elements drawn to specific features of the transmitter and receiver that can be implemented in software, these elements are not limited to software implementations. Note that [0022] discloses

> Although in the exemplary embodiment the encryption, message digest, padding and other functions are performed using software code running on the controller 120, the various functional blocks

described below may be implemented either solely in or in any combination of hardware, software, or firmware.

Similar descriptions are elsewhere in the specification.

Therefore, the non-statutory subject matter rejections are traversed.

CLAIM REJECTIONS -- 35 U.S.C. §112

Claims 2-13 were rejected under 35 U.S.C. 112, first paragraph, as based on a disclosure which is not enabling. The Examiner's rejection is based on the phrase "wherein the applying comprises" or "wherein the applying further comprises" as used in claims 2-4, and references the phrase "decrypting a payload of the data by applying" in claim 1.

First, Applicant notes that this appears to be a claim-indefiniteness rejection, as per 112, second paragraph, and not a non-enabling specification rejection under 112, first paragraph, since the rejection only discusses the claims and not the specification at all. These claims are believed to be fully supported by the specification, and the Examiner has made no allegation of lack of enabling description in the specification, so any rejection under 112, first paragraph, is traversed. Since it appears that the Examiner may have intended to make a rejection under 112, second paragraph, Applicant addresses that possibility below.

The entire relevant phrase in claim 1, truncated by the Examiner's citation, is "decrypting a payload of the data packet by applying a portion of the fixed length segment to the data packet." This language clearly indicates that the "decrypting" is performed, at least in part, by

the process of "applying a portion of the fixed length segment to the data packet." Claims 2-4, and their dependents, then further describe ways in which the "applying" process can be performed, at least in part. Applicant believes this interrelation between the "applying" process of claim 1 and the further limitations in the dependent claims to be clear and definite to those of skill in the art. As such, any rejection to these claims under 35 U.S.C. 112, second paragraph that may have been intended by the Examiner is also traversed.

Claims 4, 17, 25-32, 36, and 44 were rejected as indefinite under 35 U.S.C. 112, second paragraph, for including the trademark/trade name "RC4". As the Examiner notes, MPEP 706.03(d) indicates that "Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph" (emphasis added). The use of the term "RC4 operation" in these claims is not used to describe a particular material or product, and so does not fall under this prohibition.

While RSA Security does own a trademark (serial 74463805) for "computer software which encrypts information to conceal it during storage or transmission through use of a symmetric stream encryption algorithm," the term RC4 is widely recognized by those of skill in the art as that particular encryption algorithm, and not as a single product. The Examiner herself concedes that "the trademark/trade name is used to identify/describe a proprietary standard for stream cipher" – indicating that even the Examiner understands that the use of the term "RC4 operation" refers to a an encryption standard, not a particular piece of software from a particular

vendor.

RSA Solutions itself describes (a printout of the relevant web page is attached):

> RC4 is a stream cipher designed by Rivest for RSA Data Security (now RSA Security). It is a variable key-size stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation. Analysis shows that the period of the cipher is overwhelmingly likely to be greater than 10100. Eight to sixteen machine operations are required per output byte, and the cipher can be expected to run very quickly in software. Independent analysts have scrutinized the algorithm and it is considered secure.
>
> RC4 is used for file encryption in products such as RSA SecurPC (see Question 5.2.4). It is also used for secure communications, as in the encryption of traffic to and from secure web sites using the SSL protocol (see Question 5.1.2).

RSA Solution's own website indicates that "RC4" is known as a stream cipher algorithm, which is not a "particular material or product" as per MPEP 706.03(d).

Indeed, even a quick search of the USPTO database shows that multiple issued patents include claims that reference RC4, using the term to refer to the well-known cipher and not to a particular material or product. As such, the use of the term "RC4 operation" in the above claims

is believed to be clear, definite, and unambiguous to those of skill in the art.

CLAIM REJECTIONS -- 35 U.S.C. §102

Claims 1-5, 17-17, 41-44, 49 and 53 were rejected under 35 U.S.C. §102(e) as being anticipated by Klinger (US Pat App. Pub. No. 2003/0003896, hereinafter Klinger). These rejections are traversed.

Each of the independent claims includes reference to a "session count", at least a portion of which is used in the encryption/decryption process, as described in the specification. [0033] describes that

> In the exemplary embodiment, the session counter 324 is a packet counter and each session count 331 is a packet count identifying the packet number of each encrypted data packet 312. Examples of other suitable session counts 331 include a fixed number of packet counts. A session count 331, for example, may correspond to ten data packets 312.

Nothing in Klinger teaches or suggests anything related to a session count, or any similar count determined and used as the "session count" is used herein. Certainly the paragraphs in Klinger cited by the Examiner do not – for example, the Examiner refers to Klinger's paragraphs 0043-0046 as anticipating the first limitation of Claim 1, which includes "selecting a fixed length segment of a continuous decryption key stream based on a received session count of a data packet." Nothing in the cited description indicate that a segment of a key stream is selected based on a received session count, or anything similar to it. Nor does any such teaching appear anywhere else in Klinger.

Applicant notes that the Klinger application was filed on December 19, 2001, after the June 12, 2001 filing date of the instant application, but claims priority to provisional application 60/256,668, filed on December 19, 2000, now available on public PAIR. Applicant respectfully requests that, if the Examiner maintains the rejection over Klinger, the Examiner show where each limitation of the current claims are taught or suggested in provisional application 60/256,668, the only filing that predates this application. Any new matter in Klinger's application 10/028,573 (the '896 publication) is not available as prior art to the present application.

All rejections are traversed.

CONCLUSION

As a result of the foregoing, the Applicant asserts that the remaining Claims in the Application are in condition for allowance, and respectfully requests an early allowance of such Claims.

If any issues arise, or if the Examiner has any suggestions for expediting allowance of this Application, the Applicant respectfully invites the Examiner to contact the undersigned at the telephone number indicated below or at ***manderson@davismunck.com***.

The Commissioner is hereby authorized to charge any additional fees connected with this communication or credit any overpayment to Davis Munck Deposit Account No. 50-0208.

Respectfully submitted,

DAVIS MUNCK, P.C.

Date: 4/21/5

Matthew S. Anderson
Registration No. 39,093

P.O. Box 802432
Dallas, Texas 75380
(972) 628-3600 (main number)
(972) 628-3616 (fax)
E-mail: *manderson@davismunck.com*